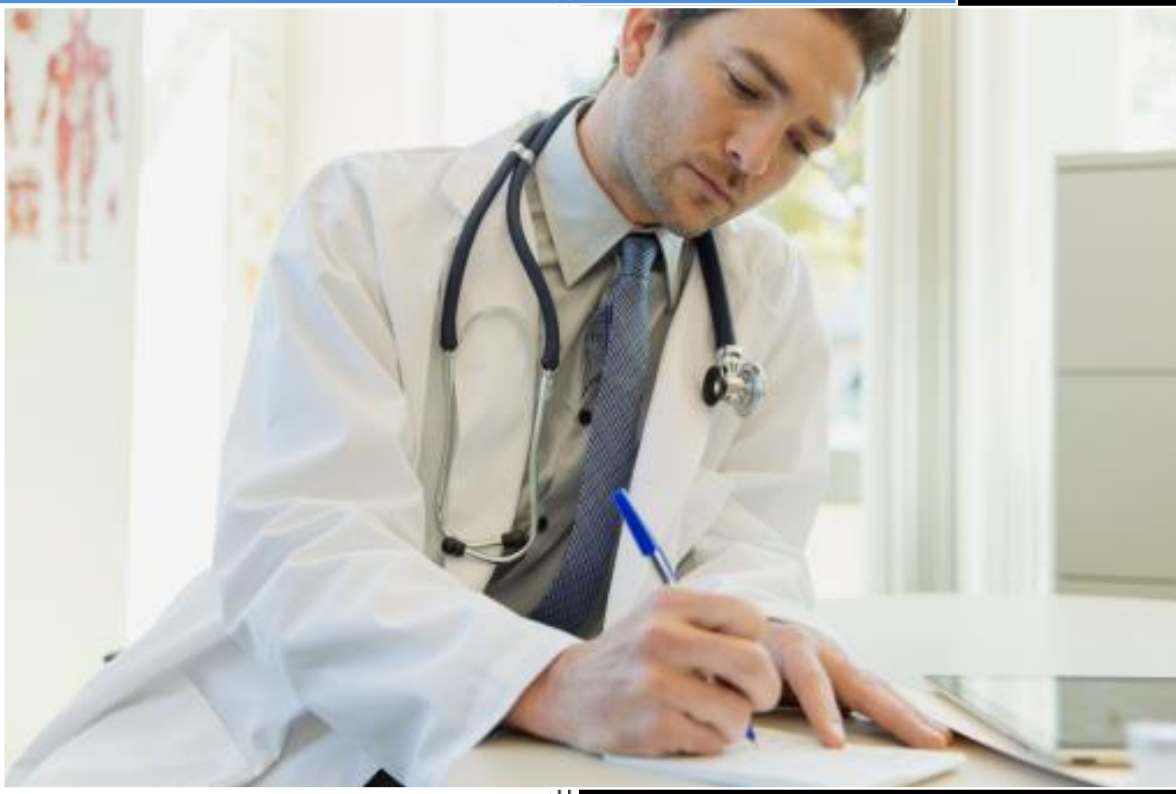
YourIT!
Your Logo Goes Here

HIPAA Assessment

HIPAA Risk Analysis



Scan Date: 4/1/2014

Prepared for:
My Client
Prepared by:
Your IT Company

4/1/2016

Table of Contents

Overview

Risk management, required by the HIPAA Security Rule, includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of ePHI and protect against any reasonably anticipated threats, hazards, or disclosures of ePHI not permitted or required under HIPAA.

After a Risk Analysis the next step in the risk management process is to develop and implement a Risk Management Plan. The purpose of a Risk Management Plan is to provide structure for the evaluation, prioritization, and implementation of risk-reducing measures and controls.

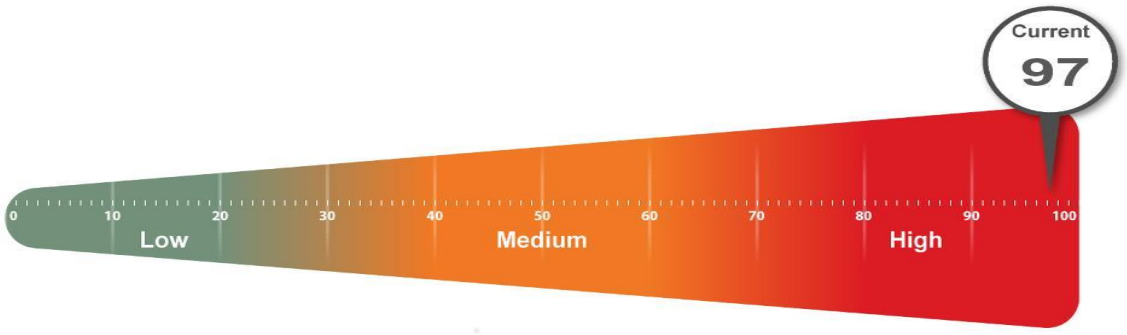
Risk prioritization and mitigation decisions will be determined by answering which controls and measures should be implemented and the priority in which they should be addressed based upon their "risk score." The implementation components of the plan include:

- Risk score (threat and vulnerability combinations) assigned to a particular issue being addressed;
- Recommendation(s) of measures and controls selected to reduce the risk of an issue;
- Ongoing evaluation and monitoring of the risk mitigation measures.

Risk analysis and risk management are not one-time activities. Risk analysis and risk management are dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management process to reduce newly identified or updated risk levels to reasonable and appropriate levels.

Risk Score

The Risk Score is a value from 0 to 100, where 100 represents significant risk and potential issues.

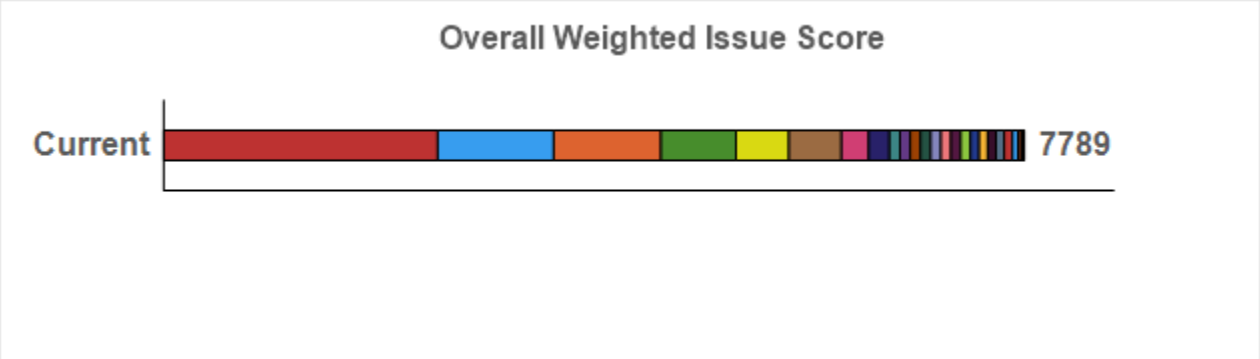


Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

If additional information is needed, please consult the Evidence of HIPAA Compliance.

Issues Summary

This section contains a summary of issues detected during the HIPAA Assessment process, and is based on industry-wide best practices for network health, performance, and security. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.



Weighted Score: Risk Score x Number of Incidents = Total points: Total percent (%)

	User password set to never expire (80 pts each)
2480	***Current Score:*** 80 pts x 31 = 2480 : 31.84%
	Requirement: §164.308(a)(5)(ii)(d): Security Awareness and Training - Procedures for creating, changing, and safeguarding passwords.
	Issue: User accounts with passwords set to never expire present a risk of use by unauthorized users. They are more easily compromised than passwords that are routinely changed.
	Recommendation: Investigate all accounts with passwords set to never expire and configure them to expire regularly.

	Significantly high number of Domain Administrators (35 pts each)
1050	***Current Score:*** 35 pts x 30 = 1050 : 13.48%
	Requirement: 45 CFR §164.308(a)(3) - Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
	Issue: More than 30% of the users are in the Domain Administrator group and have unfettered access to files and system resources. Compromised Domain Administrator accounts pose a higher threat than typical users and may lead to a breach.
	Recommendation: Evaluate the need to have more than 30% of users in the Domain Administrator group and limit administrative access to the minimum necessary.

	Unsupported Operating Systems (97 pts each)
970	***Current Score:*** 97 pts x 10 = 970 : 12.45%
	Requirement: §164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting malicious software.
	Issue: 10 computers were found using an operating system that is no longer supported. Unsupported operating systems no longer receive vital security patches and present an inherent risk.

Recommendation: Upgrade or replace computers with operating systems that are no longer supported.

	Non-administrative generic logons have access to Network Share on system with ePHI (85 pts each)
680	***Current Score:*** 85 pts x 8 = 680 : 8.73%
	Requirement: §164.308(a)(3) Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
	Issue: Generic accounts which could be in use by multiple people cannot be properly restricted and should not have access to network shares with ePHI.
	Recommendation: Remove access to Network Shares on systems with ePHI.

	Unrestricted network share with ePHI (80 pts each)
480	***Current Score:*** 80 pts x 6 = 480 : 6.16%
	Requirement: §164.308(a)(4) Information Access Management - Implement policies and procedures for authorizing access to electronic protected health information.
	Issue: Network shares containing ePHI were found as completely unrestricted (granting access to 'Everyone').
	Recommendation: Investigate the network shares containing ePHI with unrestricted access. Limit access to the minimum necessary.

	User not logged in in 90 days (not terminated) (25 pts each)
475	***Current Score:*** 25 pts x 19 = 475 : 6.1%
	Requirement: §164.308(a)(3)(ii)(C): - Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).
	Issue: Inactive user accounts were found that could potentially indicate terminated employees or vendors.
	Recommendation: Investigate all inactive accounts and disable accounts from terminated employees and vendors.

	User has not logged in in 30 days (13 pts each)
247	***Current Score:*** 13 pts x 19 = 247 : 3.17%
	Requirement: §164.308(a)(3)(ii)(C): - Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).
	Issue: Users that have not logged in in 30 days could be from a former employee or vendor and should be disabled or removed.
	Recommendation: Disable or remove user accounts for users that have not logged in in 30 days.

	Automatic screen lock not turned on. (94 pts each)
188	***Current Score:*** 94 pts x 2 = 188 : 2.41%
	Requirement: §164.312(a)(1) Access Control - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

	Issue: Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enabled allows unauthorized access to network resources.
	Recommendation: Enable automatic screen lock on the specified computers.

	Anti-spyware not installed (94 pts each)
94	***Current Score:*** 94 pts x 1 = 94 : 1.21%
	Requirement: §164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting malicious software.
	Issue: Malware protection is required but not identified as being installed on computers in the network.
	Recommendation: Install a commercial grade anti-spyware program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report.

	Anti-virus not installed (94 pts each)
94	***Current Score:*** 94 pts x 1 = 94 : 1.21%
	Requirement: §164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting malicious software.
	Issue: Malware protection is required but not identified as being installed on computers in the network.
	Recommendation: Install a commercial grade anti-virus program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report.

	Potential free hosted web-based email solution in use (93 pts each)
93	***Current Score:*** 93 pts x 1 = 93 : 1.19%
	Requirement: §164.308(b)(1): Business Associate Contracts and Other Arrangements - Covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in $160.103. The covered entity must obtain satisfactory assurance from the business associate that it will appropriately safeguard the information in accordance with §164.314(a)(1) standards.
	Issue: The use of free hosted web-based email may allow transmission of ePHI outside of the company through entities that you may not have a signed Business Associate agreement.
	Recommendation: Identify the necessity of using the free hosted email services and discontinue their use.

	Anti-spyware not turned on (92 pts each)
92	***Current Score:*** 92 pts x 1 = 92 : 1.18%
	Requirement: §164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting malicious software.
	Issue: Malware protection is required but not identified as being enabled on computers in the network.
	Recommendation: Enable anti-spyware program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report.

	Anti-virus not turned on (92 pts each)
92	***Current Score:*** 92 pts x 1 = 92 : 1.18%
	Requirement: §164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting malicious software.
	Issue: Malware protection is required but not identified as being enabled on computers in the network.
	Recommendation: Enable anti-virus program on the computers indicated in the Endpoint

Security section of the Evidence of HIPAA Compliance report.

	Anti-spyware not up to date (90 pts each)
90	***Current Score:*** 90 pts x 1 = 90 : 1.16%
	Requirement: §164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting malicious software.
	Issue: Out-of-date definitions may not properly protect a computer from attacks by malicious software.
	Recommendation: Ensure anti-spyware programs on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report are up-to-date.

	Anti-virus not up to date (90 pts each)
90	***Current Score:*** 90 pts x 1 = 90 : 1.16%
	Requirement: §164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting malicious software.
	Issue: Out-of-date definitions may not properly protect a computer from attacks by malicious software.
	Recommendation: Ensure anti-virus programs on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report are up-to-date.

	Firewall does not support IPS (88 pts each)
88	***Current Score:*** 88 pts x 1 = 88 : 1.13%
	Requirement: §164.308(a)(4): Implement policies and procedures for granting access to electronic protected health information; for example, through access to a workstation, transaction, program, process, or other mechanism.
	Issue: Firewalls without an Intrusion Prevention System (IPS) may not adequately protect the environment against malicious external attacks.
	Recommendation: Enable IPS on firewalls or investigate putting in place a firewall with IPS capabilities.

	Workstations with ePHI not backed up (78 pts each)
78	***Current Score:*** 78 pts x 1 = 78 : 1%
	Requirement: §164.308(a)(7)(ii)(A) - Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. Contingency Plan §164.308(a)(7)(ii)(b) - Establish (and implement as needed) procedures to restore any loss of data.
	Issue: Security Center reports that computers identified as having ePHI are not backed up.
	Recommendation: Ensure that data is properly backed up on computers with ePHI. See the Endpoint Security section of the Evidence of HIPAA Compliance for a list of computers.

	Account lockout disabled (77 pts each)
77	***Current Score:*** 77 pts x 1 = 77 : 0.99%
	Requirement: §164.308(a)(5)(ii)(d): Security Awareness and Training - Procedures for creating, changing, and safeguarding passwords.
	Issue: Account lockout (disabling an account after a number of failed attempts) significantly reduces the risk of an attacker acquiring a password through a brute force attack.
	Recommendation: Enable account lockout for all users.

	USB drives detected in use (unencrypted) (75 pts each)

75	***Current Score:*** 75 pts x 1 = 75 : 0.96%
	Requirement: §164.312(a)(2)(iv) Implement a mechanism to encrypt and decrypt electronic protected health information.
	Issue: Theft is the most common form of data breach. Unencrypted USB drives in an environment with ePHI may allow data loss through theft.
	Recommendation: Eliminate the use of unencrypted USB drives.

	Passwords less than 6 characters allowed (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75 : 0.96%
	Requirement: §164.308(a)(5)(ii)(d): Security Awareness and Training - Procedures for creating, changing, and safeguarding passwords.
	Issue: Passwords are not required to be 6 or more characters, allowing users to pick extremely short passwords which are vulnerable to brute force attacks.
	Recommendation: Enable enforcement of password length to 6 more characters.

	Password complexity not enabled (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75 : 0.96%
	Requirement: §164.308(a)(5)(ii)(d): Security Awareness and Training - Procedures for creating, changing, and safeguarding passwords.
	Issue: Enforcing password complexity limits the ability of an attacker to acquire a password through brute force.
	Recommendation: Enable password complexity to assure domain account passwords are secure.

	USB drives detected in use (50 pts each)
50	***Current Score:*** 50 pts x 1 = 50 : 0.64%
	Requirement: §164.312(a)(2)(iv) Implement a mechanism to encrypt and decrypt electronic protected health information.
	Issue: The use of USB drives increases the chance of data loss through theft and should be discouraged to the extent possible.
	Recommendation: Reduce or eliminate the use of USB drives in the environment.

	Audit user login in not turned on (30 pts each)
30	***Current Score:*** 30 pts x 1 = 30 : 0.39%
	Requirement: §164.308(a)(1)(ii)(D): Security Management Process - Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	Issue: Login auditing is required for proper identification of access to computers and resources. In the event of a breach, audit logs can be used to identify unauthorized access and the severity of the breach.
	Recommendation: Enable user login auditing.

	Firewall does not have malware filtering (14 pts each)
14	***Current Score:*** 14 pts x 1 = 14 : 0.18%
	Requirement: §164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting malicious software.
	Issue: Firewall malware filtering is recommended for increase protection against malicious software.
	Recommendation: Enable malware filtering on firewalls or investigate putting in place a firewall with malware filtering services.

	Computer with ePHI does not have object level auditing on (11 pts each)
11	***Current Score:*** 11 pts x 1 = 11 : 0.14%
	Requirement: §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
	Issue: Object level auditing helps identify users who have accessed files and other system resources. Object level auditing may impose an unacceptable performance impact and should be considered for use on high risk computers or environments.
	Recommendation: Evaluate the pros and cons of enabling object level access or ensure alternative methods for breach identification are in place.

	Use of generic logins (1 pts each)
1	***Current Score:*** 1 pts x 1 = 1 : 0.01%
	Requirement: §164.308(a)(1)(ii)(D): Security Management Process - Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	Issue: While not inherently a risk, the use of generic logins (logins used by more than one person or anonymous individuals) should be discouraged.
	Recommendation: Evaluate the necessity of generic logins and reduce their use when possible.